This document is scheduled to be published in the Federal Register on 08/27/2021 and available online at **federalregister.gov/d/2021-18533**, and on **govinfo.gov**

[9110-05-P]

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

Intent to Request an Extension from OMB of One Current Public Collection of Information: Pipeline Corporate Security Review Program

AGENCY: Transportation Security Administration, DHS.

ACTION: 60-day notice.

SUMMARY: The Transportation Security Administration (TSA) invites public comment on one currently-approved Information Collection Request (ICR), Office of Management and Budget (OMB) control number 1652–0056, abstracted below, that we will submit to OMB for an extension in compliance with the Paperwork Reduction Act (PRA). On July 15, 2021, OMB approved TSA's request for an emergency revision of this collection to address the ongoing cybersecurity threat to pipeline systems and associated infrastructure. TSA is now seeking to renew the collection, which expires on January 31, 2022, with incorporation of the subject of the emergency revision. The ICR describes the nature of the information collection and its expected burden. The collection allows TSA to assess the current security practices in the pipeline industry through TSA's Pipeline Corporate Security Review (PCSR) program. The PCSR program is part of the larger domain awareness, prevention, and protection program supporting TSA's and the Department of Homeland Security's missions.

DATES: Send your comments by **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].**

ADDRESSES: Comments may be e-mailed to TSAPRA@tsa.dhs.gov or delivered to the TSA PRA Officer, Information Technology (IT), TSA-11, Transportation Security Administration, 6595 Springfield Center Drive, Springfield, VA 20598-6011.

FOR FURTHER INFORMATION CONTACT: Christina A. Walsh at the above address, or by telephone (571) 227-2062.

SUPPLEMENTARY INFORMATION:

Comments Invited

In accordance with the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*), an agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid OMB control number. The ICR documentation will be available at http://www.reginfo.gov upon its submission to OMB. Therefore, in preparation for OMB review and approval of the following information collection, TSA is soliciting comments to--

(1) Evaluate whether the proposed information requirement is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;

(2) Evaluate the accuracy of the agency's estimate of the burden;

(3) Enhance the quality, utility, and clarity of the information to be collected; and

(4) Minimize the burden of the collection of information on those who are to respond, including using appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology.

Information Collection Requirement

OMB Control Number 1652-0056; Pipeline Corporate Security Review (PCSR) Program. Under the Aviation and Transportation Security Act[1] and delegated authority from the Secretary of Homeland Security, TSA has broad responsibility and authority for "security in all modes of transportation . . . including security responsibilities . . . over modes of transportation that are exercised by the Department of Transportation."[2] TSA is

---

[1] Pub. L. 107-71 (115 Stat. 597; Nov. 19, 2001), codified at 49 U.S.C. 114.

[2] *See* 49 U.S.C. 114(d). The TSA Administrator's current authorities under the Aviation and Transportation Security Act have been delegated to him by the Secretary of Homeland Security. Section

specifically empowered to assess threats to transportation;[3] develop policies, strategies, and plans for dealing with threats to transportation;[4] oversee the implementation and adequacy of security measures at transportation facilities;[5] and carry out other appropriate duties relating to transportation security.[6] The Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act) included a specific requirement for TSA to conduct assessments of critical pipeline facilities.[7]

Assessing Voluntary Implementation of Recommendations

Consistent with these authorities and requirements, TSA developed the PCSR program to assess the current security practices in the pipeline industry, with a focus on the physical and cyber security of pipelines and the crude oil and petroleum products, such as gasoline, diesel, jet fuel, home heating oil, and natural gas, moving through the system infrastructure. PCSRs are voluntary, face-to-face visits, usually at the headquarters facility of the pipeline owner/operator. Typically, TSA sends one to three employees to conduct a seven to eight hour interview with representatives from the owner/operator. The TSA representatives analyze the owner/operator's security plan and policies and compare their practices with recommendations in TSA's Pipeline Security Guidelines.

During the PCSR assessment, the PCSR program subject matter experts:

- Meet with senior corporate officers and security managers.
- Develop knowledge of security planning at critical pipeline infrastructure sites.

403(2) of the Homeland Security Act (HSA) of 2002, Pub. L. 107-296 (116 Stat. 2135, Nov. 25, 2002), transferred all functions of TSA, including those of the Secretary of Transportation and the Under Secretary of Transportation of Security related to TSA, to the Secretary of Homeland Security. Pursuant to DHS Delegation Number 7060.2, the Secretary delegated to the Administrator of TSA, subject to the Secretary's guidance and control, the authority vested in the Secretary with respect to TSA, including that in section 403(2) of the HSA.

[3] 49 U.S.C. 114(f)(2).

[4] 49 U.S.C. 114(f)(3).

[5] 49 U.S.C. 114(f)(11).

[6] 49 U.S.C. 114(f)(15).

[7] *See* section 1557 of Pub. L. 110-53 (121 Stat. 266; Aug. 3, 2007) as codified at 6 U.S.C. 1207.

- Establish and maintain a working relationship with key security staff who operate critical pipeline infrastructure.
- Identify industry smart practices and lessons learned.
- Maintain a dynamic modal network through effective communications with the pipeline industry and government stakeholders.

Through this engagement, TSA is also able to establish and maintain productive working relationships with key pipeline security personnel. This engagement and access to pipeline facilities also enables TSA to identify and share smart security practices observed at one facility to help enhance and improve the security of the pipeline industry. As a result, participation in the voluntary PCSR program enhances pipeline security at both specific facilities and across the industry.

TSA has developed a Question Set to aid in the conducting of PCSRs. The PCSR Question Set structures the TSA-owner/operator discussion and is the central data source for the security information TSA collects. TSA developed the PCSR Question Set based on input from government and industry stakeholders on how best to obtain relevant information from a pipeline owner/operator about its security plan and processes. The questions are designed to examine the company's current state of security, as well as to address measures that are applied if there is a change in the National Terrorism Advisory System. The PCSR Question Set also includes sections for facility site visits and owner/operator contact information. By asking questions related to specific topics (such as security program management, vulnerability assessments, components of the security plan, security training, and emergency communications), TSA is able to assess the strength of owner/operator's physical security, cyber security, emergency communication capabilities, and security training.

This PCSR information collection provides TSA with real-time information on a company's security posture. The relationships these face-to-face contacts foster are

critical to the Federal government's ability to reach out to the pipeline stakeholders affected by the PCSRs. In addition, TSA follows up via email with owner/operators on specific recommendations made by TSA during the PCSR.

When combined with information from other companies across the sector, TSA can identify and develop recommended smart practices and security recommendations for the pipeline mode. This information allows TSA to adapt programs to the changing security threat, while incorporating an understanding of the improvements owners/operators make in their security measures. Without this information, the ability of TSA to perform its security mission would be severely hindered.

Establishing Compliance with Mandatory Requirements (Emergency Revision)

While the above listed collections are voluntary, on July 15, 2021, OMB approved TSA's request for an emergency revision of this information collection, allowing for the institution of mandatory requirements. *See* ICR Reference Number: 202107-1652-002. TSA is now seeking renewal of this information collection for the maximum three-year approval period.

The revision was necessary as a result of actions TSA took to address the ongoing cybersecurity threat to pipeline systems and associated infrastructure. On July 19, 2021, TSA issued a Security Directive (SD) applicable to owners/operators of critical hazardous liquid and natural pipelines and liquefied natural gas facilities.[8] These owners/operators are required to develop and adopt a Cybersecurity Contingency/Response Plan to ensure the resiliency of their operations in the event of a cybersecurity attack. Owners/operators must provide evidence of compliance to TSA

[8] On May 28, 2021, TSA issued another SD which included three information collections. OMB control number 1652-0055, includes two of these information collections, requiring owner/operators to report cybersecurity incidents to CISA, and to designate a Cybersecurity Coordinator, who is required to be available to the TSA 24/7 to coordinate cybersecurity practices and address any incidents that arise, and who must submit contact information to TSA. OMB control number 1652-0050 contains the remaining information collection, requiring owner/operators to conduct a cybersecurity assessment, to address cyber risk, and identify remediation measures that will be taken to fill those gaps and a time frame for achieving those measures..

upon request. In addition, owner/operators are required to have a third-party complete an evaluation of their industrial control system design and architecture to identify previously unrecognized vulnerabilities. This evaluation must include a written report detailing the results of the evaluation and the acceptance or rejection of any recommendations provided by the evaluator to address vulnerabilities. This written report must be made available to TSA upon request and retained for no less than 2 years from the date of completion. Finally, within 7 days of each deadline set forth in the SD, owner/operators must ensure that their Cybersecurity Coordinator or other accountable executive submits a statement to TSA via email certifying that the owner/operator has met the requirements of the SD. For convenience, TSA will provide an optional form (TSA Security Directive Pipeline 2021-02 Statement of Completion) for each submission deadline that owner/operators can complete and submit via email. This form is Sensitive Security Information (SSI) and will only be shared with the owner/operators and others with the need to know. TSA requires that certifications be made in a timely way. Documentation of compliance must be provided upon request.

Portions of PCSR responses that are deemed SSI are protected in accordance with procedures meeting the transmission, handling, and storage requirements of SSI set forth in parts 15 and 1520 of title 49, Code of Federal Regulations (CFR). Information developed and submitted pursuant to TSA's SD is also SSI.

The annual hour burden for the voluntary information collection is estimated to be 220 hours based upon 20 PCSR visits per year, each lasting a total of eight hours and the follow-up regarding security recommendations, lasting up to three hours, ((20 x 8 = 160 hours) + (20 x 3 = 60 hours) = 220 hours).

For the mandatory information collection, TSA estimates a total of 97 owner/operators will provide the responses for the Cybersecurity Contingency/Response

Plan; Third-Party Evaluation; and Certification of Completion. TSA estimates the total annual burden hours for the mandatory collection to be 12,610 hours.

TSA estimates that it will take approximately 80 hours to complete the response for the Cybersecurity Contingency/Response Plan, totaling 7,760 hours (97 respondents x 80 hours = 7,760 hours). In addition, TSA estimates that it will require approximately 42 hours to complete the Third-Party Evaluation, totaling 4,074 hours (97 respondents x 42 hours = 4,074 hours). Finally, TSA estimates that it will take eight (8) hours to complete the Certification of completion of SD requirements, totaling 776 hours (97 respondents x 8 hours = 776 hours). Thus, the total annual burden hours for the mandatory collection is 12,610 hours (7,760 + 4,074 + 776 = 12,610).

TSA estimates the total respondents for the information collection is 97 and the combined annual burden hours for the voluntary and mandatory collections are 12,830 hours (220 + 7,760 + 4,074 + 776 = 12,830).

Dated: August 24, 2021.

Christina A. Walsh,

TSA Paperwork Reduction Act Officer,

Information Technology.

[FR Doc. 2021-18533 Filed: 8/26/2021 8:45 am; Publication Date: 8/27/2021]